

CITY OF SAN ANTONIO



Administrative Directive

AD 7.8C Remote Access

Procedural Guidelines

Guidelines to establish security parameters for remote access to the City network.

Department/Division

Information Technology Services Department (ITSD)

Effective Date

July 6, 2009

Project Manager

John Byers, Chief Information Security Officer (CISO)

Purpose

This directive is designed to minimize the potential exposure to the City from damages that may result from the unauthorized use of City resources. Damages include the loss of sensitive or confidential data, intellectual property, damage to public image, or damage to critical information technology (IT) systems.

Policy

This document describes the directive under which City of San Antonio (COSA) employees, contractors, vendors, and third party organizations may connect to COSA networks for transacting business related to the City.

Policy Applies To

☐ External & Internal Applicants

☒ Current Temporary Employees

☒ Current Full-Time Employees

☐ Current Volunteers

☒ Current Part-Time Employees

☒ Current Grant-Funded Employees

☒ Current Paid and Unpaid Interns

☒ Police and Fire Academy Trainees

☒ Uniformed Employees Under Collective Bargaining Agreements

Definitions

N/A

Policy Guidelines

General Guidelines:

A. This directive applies to all COSA employees, contractors, vendors, and agents who connect to the City network to do work on behalf of

the City, including but not limited to, reading or sending email, accessing and viewing intranet web resources, performing system administrative functions, and/or providing support to City systems and infrastructure.

- B. Remote access implementations that are covered by this directive include, but are not limited to, dial-in modems, frame relay, integrated services digital network (ISDN), digital subscriber line (DSL), virtual private network (VPN), secure shell (SSH), and cable modems, wireless or any other means by which connection is made to the City.
- C. In accordance with *AD 7.5, Acceptable Use of Information Technology* (http://www.sanantonio.gov/hr/admin_directives), any use that occurs under an employee's login is presumed to be performed by that employee.
- D. A user who is granted remote access privileges must remain aware that connections between their location and the City are literal extensions of the City network that provide a potential path to the City's sensitive information. The employee and/or authorized third party individual must take every reasonable measure to protect City assets.
- E. Secure remote access control shall be enforced utilizing the current technologies available and approved for access control. This may include, but is not limited to, one-time password authentication, public/private keys with strong pass-phrases, use of biometrics, or security tokens. The minimum requirement is the use of complex passwords as outlined in *AD 7.6 Security and Passwords* (http://www.sanantonio.gov/hr/admin_directives).
- F. Remote access connectivity shall be configured to prevent split-tunneling or dual homing.
- G. Effective January 1, 2010, all systems and devices that connect to the City via remote access must use anti-virus (AV) software. The anti-virus software must be maintained to ensure that it is current.
- H. Remote access accounts are not automatically created and must be requested by the appropriate departmental manager. Each department shall determine the proper authority for request and approving for the department. At a minimum, the request should be approved by the employee's manager. The same account restrictions, activity, provisioning and de-provisioning that govern normal accounts apply to remote access.

Third Parties, Contractors, and Vendors

- I. All new connectivity must go through a security review. This may include a site visit of the third party's facilities. Additional information may be required from the third party.
- J. All connection requests between third parties and the City shall

require that the third party agree to comply with the requirements of this directive.

- K. The third party agreement must be signed by a representative of the third party who is legally empowered to sign on behalf of the third party and the sponsoring City Department. The signed document pertaining to remote access shall be maintained by the sponsoring City Department and a copy will be kept on file at ITSD.
- L. The employee of the third party connecting remotely to City networks must complete a criminal background check. Criminal background checks are standard practice for government organizations whether local, State, or Federal. The background check looks for criminal activity, arrests, convictions, warrants, and other information that is normally associated with a criminal background. Background checks aid in establishing trust for a business or individual that provides services to the City. The City has the responsibility to establish "Public Trust" to ensure a safe and secure workplace and to safeguard the technologies and information of the City.
- M. The City accepts the following as acceptable "authorities" for background checks:
 - 1. Criminal background checks shall include all local, State and Federal criminal justice databases. Additionally, a person(s) that will or could have access to sensitive systems or information shall also submit fingerprints as required by Federal guidelines.
 - 2. Active US Department of Defense (DOD) security clearance.
 - 3. Active US Government clearance issued by a Department or Agency of the US Federal government.
 - 4. State of Texas active and valid background check or current security clearance issued by the State of Texas.
 - 5. Company criminal background check conducted on the employee within the last two (2) years must include a National criminal background check. A copy for verification must accompany the Request for Remote Access Form.
- N. All requests for access to a production environment must be justified in writing as required by the COSA Remote Access Form (see Attachments). The justification is the responsibility of the COSA department requesting the third-party access.
- O. All remote connectivity by third parties should be granted based on a pre-approved and pre-defined time limit, for example 24 hours, one week, or one month. The remote account should expire automatically at the end of the pre-approved period.
- P. In keeping with industry best practices, third party accounts not used for a period of 30 days without prior notification will be suspended.

If remote access is subsequently required, the individual must request a reactivation. Accounts that have been suspended and reactivation not requested for a period of 60 days shall be terminated.

- Q. An electronic copy of this directive may be provided to third parties, contactors, or vendors.

Roles & Responsibilities

Chief Information Security Officer

- A. Review this directive annually, at a minimum, for both consistency and accuracy
- B. Interpret and apply this directive under the direction of the Chief Information Officer (CIO) and/or the Chief Technology Officer (CTO), as appropriate
- C. Modify or amend this directive at any time pending formal review and approval as defined in *AD 7.5A Establishing IT-Related Directives*
- D. Provide adequate notice of any such modifications or amendments
- E. Ensure the current version of this directive is posted in a public location accessible to all authorized City personnel
- F. Communicate the standards established in this directive to all third-party users and for ensuring their compliance
- G. Review connectivity requests and either approve, or disapprove, or recommend changes

ITSD

- A. Take immediate appropriate action to resolve the issue should a security incident or audit finding reveal that a circuit has been compromised

Employees

- A. Ensure that a connection to COSA is not used by non-City authorized persons to gain access to City information system resources
- B. Remove all software, data, or other enabling technology provided by the City for the purpose of the remote access if access is no longer required

Departments

- A. Responsible for any disciplinary action taken against employees who violate this directive
- B. Responsible for identifying the third-party users to ITSD
- C. prevent the unauthorized use of the City's communications systems while logged into the City's network
- D. Review employee remote access on a monthly basis
- E. Notify ITSD by contacting the ITSD Service Desk (7-8888) or through the normal employee termination or retirement process to

	<p>terminate employee access if the connectivity for any employee is no longer required</p> <p>F. Designate a person to be the point-of-contact (POC) who shall act on behalf of the department and will be responsible for those portions of this directive and the third party</p> <p>G. File a new site request with the ITSD to establish connectivity to a third party providing full and complete information as to the nature of the proposed access</p> <p>H. Address security issues inherent in projects</p>
<u>Human Resources</u>	A. Provide guidance, as required, to City departments regarding appropriate disciplinary action to be taken against employees who violate this directive
Attachments	
<u>Attachment 1</u>	<u>Remote Access Request Form</u>

Information and/or clarification may be obtained by contacting the Information Technology Services Department (ITSD) at 207-8301.

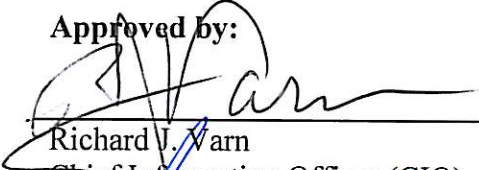


 Hugh Miller
 Information Technology Services Department Director / CTO

09/14/2009

 Date

Approved by:




 Richard J. Warr
 Chief Information Officer (CIO)

09/16/2009

 Date

Approved by:



 Sheryl Sculley
 City Manager

9-29-09

 Date